

DOCKET NO.: IVPH-0049



PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of:

**Laurence Hamid, Derek Christopher  
Bouius and Albert Hum**

Confirmation No.: 1343

Application No.: 09/863,301

Group Art Unit: 2135

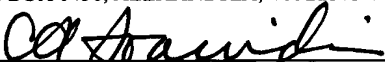
Filing Date: May 24, 2001

Examiner: **Thanhnga B. Truong**

For: **METHOD AND SYSTEM FOR PROVIDING GATED ACCESS FOR A  
THIRD PARTY TO A SECURE ENTITY OR SERVICE**

DATE OF DEPOSIT: June 12, 2006

I HEREBY CERTIFY THAT THIS PAPER IS BEING  
DEPOSITED WITH THE UNITED STATES POSTAL  
SERVICE AS FIRST CLASS MAIL, POSTAGE PREPAID,  
ON THE DATE INDICATED ABOVE AND IS  
ADDRESSED TO THE COMMISSIONER FOR PATENTS,  
P.O. BOX 1450, ALEXANDRIA, VA 22313-1450.

  
TYPED NAME: Christos A. Ioannidi  
REGISTRATION NO.: 54,195

Mail Stop Appeal-Brief Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

**APPELLANT'S BRIEF PURSUANT TO 37 C.F.R. § 41.37**

This brief is being filed in support of Appellant's appeal from the rejections of claims 1-20 in the Final Rejection mailed August 24, 2005. A Notice of Appeal was filed on February 24, 2006.

**1. REAL PARTY IN INTEREST**

The real party in interest is **ActivCard Ireland Limited**, as assignee of the inventors' rights.

**2. RELATED APPEALS AND INTERFERENCES**

None.

06/16/2006 MAHMED1 00000015 09863301

01 FC:1402

500.00 OP

### 3. STATUS OF CLAIMS

Claims 1-20 are rejected and are the subject of this appeal. Claims 1, 4, 11 and 15 are independent.

### 4. STATUS OF AMENDMENTS

No claim amendment has been entered subsequent to the Final Rejection. The proposed minor amendment to claim 15 is hereby withdrawn.

### 5. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter includes a biometric security system that provides gated access for third parties to a secure entity or service. For example, an embodiment of the claimed invention may permit a handheld biometric identification device (*e.g.*, fingerprint scanner) to allow an authorized user to provide gated access for a third party to a secure entity or service. As described in the example in paragraph [0045] of the specification, a stockbroker may desire to provide access to a computer network for his assistants but only during his presence. Using the handheld biometric identification device, he may provide a gating signal to the security system that enables the system to respond to signals provided by his assistant. The assistant may then send his or her own biometric identification signal to the security system to gain access. Without the gating signal, the assistant may not have access.

In the embodiment of Figure 1 (described in paragraph [0030] in the specification), biometric security system 100 includes a portable biometric device 102 and a receiving module 104 connected thereto via a transmission channel that may be a wireless transmission channel, such as an infrared or radio frequency transmission channel. Generally, each user has a portable biometric device 102 that communicates with the receiving module 104. The portable biometric device 102 may be a small handheld device such as a remote control, a watch a pendant or a smart card (see paragraph [0034] of the specification) and may include a biometric sensor 106 that captures biometric information, such as a fingerprint, of a user and an encoder 108 that digitizes or otherwise converts the analog signal into an encoded signal format for further processing. A processor 110 compares the captured biometric data with biometric data of the authorized user stored in memory 112 to produce a comparison result. If the comparison result is indicative of a match, a gating signal for enabling signals

generated by third parties to access the secure entity or service protected by the biometric security system 100 is generated and transmitted by transmitter 114 over the transmission channel to a receiving port of the receiving module 104. In response to the gating signal, a processor 124 of a locking mechanism 122 sets a flag that, when set, permits signals from the third parties to be received and processed. The flag has two states: a first state in which the locking mechanism 122 is non-responsive to signals from the third parties and a second state in which the locking mechanism 122 is responsive to the signals from the third parties. Of course, if the comparison result is not indicative of a match, the locking mechanism 122 remains in the non-responsive state. The flag's state may be changed back from the second state to the first state by providing a second gating signal and/or the flag may return to the non-responsive state (first state) after a predetermined amount of time (see paragraph [0039] of the specification).

The biometric data of a particular third party may be stored in a memory of the biometric device 102 to restrict third party access to a particular third party (see paragraph [0031] of the specification). Also, the locking mechanism 122 may include a memory 126 that stores data indicative of access privileges for respective third parties so that various levels of access privileges for the third parties may be provided (see paragraph [0032] of the specification). In another alternate embodiment, the signals provided by different persons may be received at different ports 120 of the receiving module 104 (see paragraph [0033] of the specification). Also, as described in paragraphs [0043]-[0044] of the specification with respect to Figures 4a and 4b, the third parties may have portable biometric devices that provide signals that are accepted by the locking mechanism 122 only when the flag is set to the responsive state (second state). The third parties may have different access privileges such that different signals are provided by their portable biometric device than the signals provided for other persons with different access privileges.

## **6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

Claim 1 stands finally rejected under 35 U.S.C. 102(e) as allegedly being anticipated by Li et al. (US 6,219,793).

Claims 2-20 stand finally rejected under 35 U.S.C. 103(a) as allegedly being obvious over Li et al. (US 6,219,793) in view of Diamant et al. (US 5,969,632).

These rejections are believed to be improper and are the subject of this appeal.

**7. ARGUMENT**

Withdrawal of the Final Rejection is requested for the following reasons:

**1. Li et al. (US 6,219,793) do not anticipate claim 1 since Li et al. do not teach or suggest "providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service said access provided for a predetermined, limited period of time" as claimed.**

Li et al. disclose a system in which a mobile telephone 102 includes a fingerprint scanner and an authenticated fingerprint from the user is required to authorize a wireless communication. In this fashion, only calls from authorized users are connected. In contrast, claim 1 relates to a method by which a first designated user provides gated access for *a third party* to a secure entity or service. In other words, a first designated user authorizes gated access by a different person to the secure entity or service for a limited period of time. Further security may also require that the third party be an authorized user. This third party gated access is accomplished by providing the claimed "wireless gating signal." For example, as set forth in paragraph [0045] on page 15 of the specification, a stockbroker may use the claimed method to provide access to a computer network for his staff only during his presence. By contrast, Li et al.'s system is designed to enable access to the wireless network by the person who provides his or her fingerprint at the fingerprint scanner on the mobile phone. Li et al. do not discuss third party access to a secure entity or service by providing the claimed "wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service" where the access is "provided for a predetermined, limited period of time" as claimed.

The Examiner responded to Applicant's argument by alleging that the term "wireless gating signal" is "just another term to activate and/or turn on/off [sic] signal through wireless communication" and that Li et al. thus teach the claimed subject matter. However, accepting the Examiner's interpretation for the sake of argument, Li et al. still do not disclose turning on/off the access of a third party as claimed. The closest Li et al. come to this is an embodiment at column 15, lines 15-30, whereby multiple users may use the same wireless phone by storing challenge keys 202 for each user in the challenge key database at the mobile switching center. The phone owner may function as a "master user" who may allow other users to use his or her phone by activating appropriate buttons on the phone and associating the user's fingerprint with the master user's challenge key stored in the database at the mobile

switching center. In other words, the master user can remotely authorize the use of his or her mobile phone by validating the use with his or her fingerprint. The second user would then use the wireless phone by swiping his or her fingerprint and proceeding to make a call once access is granted. Applicant submits that such teachings by Li et al. also fall well short of anticipating claim 1.

In particular, while Li et al. allow a first user to authorize secure access to a wireless network by a second user, no "wireless gating signal" (or even on/off access as interpreted by the Examiner) is provided as set forth in claim 1. In fact, no access at all is provided until the second user is granted access upon fingerprint authentication and such access is not "gated" by the first user in that it may continue indefinitely. The access control is provided by "activating appropriate buttons" at the wireless phone - not by sending a wireless gating signal "enabling wireless signals provided by the third party to access the secure entity or service ... for a predetermined, limited period of time" as claimed. In Li et al., once enabled, the access by the second party would be unlimited and not "wirelessly gated" "for a predetermined, limited period of time" as claimed.

The Examiner further argues in the comments to the Advisory Action that the timestamp specifying when the user's fingerprint was taken in the Li et al. system corresponds to the claimed "gated access." Applicant disagrees. The timestamp is used to thwart attempts by third parties to intercept and improperly use the fingerprint data to gain system access. The timestamp is in no way used to gate the third party access. In fact, no third party access at all would be provided if the timestamp data indicates that there has been an attempt to gain improper access. Moreover, the timestamp in now way limits third party access to a "predetermined, limited period of time" as claimed.

Withdrawal of the rejection of claim 1 as anticipated by Li et al. is thus appropriate and is respectfully solicited.

**2. Li et al. (US 6,219,793) in view of Diamant et al. (US 5,969,632) do not render obvious the subject matter of claims 2-20 since Li et al. and Diamant et al. together do not teach or suggest "providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service" as claimed.**

As noted above, Li et al. do not teach "providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service said access provided for a predetermined, limited period of time" as claimed in independent claim 1. Diamant et al. provide no such teachings of providing a "gating signal" either. On the

contrary, Diamant et al. disclose a communication apparatus in which security flags may be set to on and off (Figure 8, steps 500 and 506) whereby a security key is provided by the user only when the security flag is on and the system is off-line, thereby eliminating unauthorized access to the security key from unauthorized on-line elements that may try to appropriate the security key. In other words, Diamant et al. functions to *preclude* third party access – not to gate such access as claimed. Applicant submits that Diamant et al. thus teach away from the claimed invention and provide no teachings of providing controlled third party access to a secure entity or service as claimed. In any case, Applicant can find no teachings in Diamant et al. that teach or suggest the missing step of Li et al., namely, "providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service." In the absence of such teachings, even if one skilled in the art would have been motivated to combine the teachings of Li et al. and Diamant et al. as the Examiner proposes, the claimed invention could not have resulted.

The Examiner acknowledges in the Final Rejection that Li et al. is "silent about setting a flag within the Central Authentication System) as shown in Figure 1, element 106" (page 4, lines 6-7). Nevertheless, the Examiner cites the teachings in Diamant et al. of setting a security flag to on and off (column 13, lines 21-42) and alleges that it would have been obvious to modify the Li et al. system to turn a security flag on and off to secure access to data and services over a network as claimed. The reason provided for this combination is that one skilled in the art would wish to modify Li et al.'s system to overcome vulnerability to hostile intrusion by unauthorized persons or data viruses. Applicant respectfully disagrees as significant features of the invention are nowhere shown or suggested by Li et al. and/or Diamant et al.

***Method Claims 2-3 Dependent Upon Independent Claim 1***

Claims 2-3 further specify that the wireless gating signal provided in claim 1 is used to set a flag within the secure entity or service that is, in turn, used to gate received wireless signals from a third party for controlling access to the secure entity or service by the third party. As noted above, Diamant et al. teach using security flags to prevent access to the user's security key by an unauthorized on-line user. By preventing access by third parties, Diamant et al. do not teach using flags for gated access as claimed. Moreover, the flags are not set to allow access for a predetermined amount of time as claimed. Accordingly, even if one skilled in the art would have known to modify the Li et al. system to turn on and off security flags, the claimed invention of claims 2 and 3 would not have resulted.

***Method Claims 4-10***

Independent claim 4 specifies that the wireless gating signal enables wireless signals provided by a third party to access the secure entity or service. Claim 4 also specifies that a flag is set within the secure entity or service to authorize in a second state or not authorize in a first state the third party to access the secure entity or service and that the flag supports a timing function “such that the flag once set to the second other state returns to the first state after a predetermined, limited period of time absent additional comparison results indicative of a match.” As noted above, Diamant et al. teach using security flags to prevent access to the user’s security key by an unauthorized on-line user. By preventing access by third parties, Diamant et al. do not teach using flags for gated access as claimed. Moreover, the flags are not set to allow access for a predetermined amount of time as claimed. Accordingly, even if one skilled in the art would have known to modify the Li et al. system to turn on and off security flags, the claimed invention of claim 4 would not have resulted.

Dependent claim 8 further specifies that different persons of a plurality of third parties have different access privileges to the secure entity or service. Applicant submits that neither Li et al. nor Diamant et al. provides any teachings of providing different access privileges to third parties. As noted above, Diamant et al. prohibit access by third parties. Li et al. disclose that multiple users may be enabled to use a phone, but the Examiner has not indicated where Li et al. specify that different users may have different access privileges as claimed. Absent such teachings, the rejection of claim 8 (and claims 9 and 10 dependent thereon) must fail.

***Method Claims 11-14***

Independent claim 11 further specifies that a first designated user and a third party are each provided with portable biometric devices and that a wireless gating signal from the first designated user’s portable biometric device provides a “wireless gating signal” that enables wireless signals provided by the third party to access the secure entity or service. Claim 11 also specifies that a flag is set within the locking mechanism to authorize in a second state or not authorize in a first state the third party to access the secure entity or service. As noted above, Diamant et al. teach using security flags to prevent access to the user’s security key by an unauthorized on-line user. By preventing access by third parties, Diamant et al. do not teach using flags for gated access as claimed. Moreover, neither Li et al. nor Diamant et al. teaches the use of portable biometric devices to provide the claimed gated access as set forth in claims 11 and 12. Accordingly, even if one skilled in the art would have known to modify

the Li et al. system to turn on and off security flags, the claimed invention of claim 11 would not have resulted.

Claim 14 further specifies that different ports may be used to receive the wireless signals from different portable biometric devices. As noted above, neither Li et al. nor Diamant et al. provides any teachings of providing wireless gating signals from portable biometric devices as claimed. Similarly, neither Diamant et al. nor Li et al. provide any teaching of using different ports to receive the signals from such portable biometric devices. The Examiner notes that Li et al. disclose that the CAS 106 may handle many calls from multiple users, but the Examiner has not indicated where Li et al. specify that multiple ports are used to receive wireless signals from multiple portable biometric devices and that the receipt of such signals is authorized by a “wireless gating signal” as claimed. Absent such teachings, the rejection of claim 14 must fail.

***Security System Claims 15-20***

Independent claim 15 recites a security system including a portable biometric device, a port for receiving a wireless gating signal from the portable biometric device, and a locking mechanism that sets a flag in response to the wireless gating signal. Claim 15 also specifies that the flag is set within the locking mechanism to authorize in a second state or not authorize in a first state the third party to access the secure entity or service. As noted above, Diamant et al. teach using security flags to prevent access to the user’s security key by an unauthorized on-line user. By preventing access by third parties, Diamant et al. do not teach using flags for gated access as claimed. Moreover, neither Li et al. nor Diamant et al. teaches the use of portable biometric devices with processors and biometric sensors that function together to provide the claimed gated access as set forth in claim 15. Accordingly, even if one skilled in the art would have known to modify the Li et al. system to turn on and off security flags, the claimed invention of claim 11 would not have resulted.

Claim 20 further specifies that the locking mechanism includes memory for storing data indicative of access privileges. As noted above, neither Li et al. nor Diamant et al. provides any teachings of providing different access privileges to third parties. As noted above, Diamant et al. prohibit access by third parties. Li et al. disclose that multiple users may be enabled to use a phone, but the Examiner has not indicated where Li et al. specify that different users may have different access privileges as claimed. Absent such teachings, the rejection of claim 20 must fail.

***Lack of Motivation to Combine Li et al. and Diamant et al.***



Given that Li et al. and Diamant et al., taken separately or together, do not teach or suggest all the claim limitations, the Examiner has not established a *prima facie* case of obviousness. Moreover, the Examiner has further failed to provide a *prima facie* case of obviousness with respect to any claim since the Examiner has not met his burden of providing a suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the reference teachings. Instead, the Examiner has provided general references to preventing "hostile intrusion by unauthorized persons or data viruses" by combining the teachings of Li et al. and Diamant et al. However, the Examiner has provided no plausible reason as to why one skilled in the art would use the security flags of Diamant et al. in a system of the type disclosed by Li et al. Applicant suggests that no such motivation exists because security flags would serve no apparent purpose in the Li et al. system where the access by a third party is not gated as claimed and need not be "flagged" as claimed. As a result, one skilled in the art would not be motivated to combine the teachings of Li et al. and Diamant et al. to provide a "wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service" as claimed.

In the absence of the requisite teachings and motivations to combine teachings to establish *prima facie* obviousness, the rejection of claims 2-20 as being obvious over Li et al. and Diamant et al. is improper and withdrawal of the obviousness rejection is respectfully solicited.

### **Conclusion**

In view of the above, Applicant submits that claims 1-20 are allowable over the art of record. Allowance of claims 1-20 is solicited.

## **8. CLAIMS APPENDIX**

1. (Previously Presented) A method for providing gated access for a third party to a secure entity or service comprising:

storing biometric data in dependence upon a biometric characteristic of a first designated user of the secure entity or service other than the third party;

capturing biometric information representative of a biometric characteristic and providing biometric data in dependence thereupon;

comparing the captured biometric data with the stored biometric data to produce a comparison result; and,

if the comparison result is indicative of a match:

providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service said access provided for a predetermined, limited period of time.

2. (Previously presented) A method of providing gated access for a third party to a secure entity or service as defined in claim 1, comprising:

receiving the gating signal at the secure entity or service;

in response to the wireless gating signal, setting a flag within the secure entity or service, the flag for use in gating received wireless signals for controlling access to the secure entity or service such that in a first state the secure entity or service is non responsive to the wireless signals and in a second other state the secure entity or service is responsive to the wireless signals provided by the third party.

3. (Original) A method for providing gated access for a third party to a secure entity or service as defined in claim 2, wherein the flag is returned to the first state after a predetermined amount of time.

4. (Previously presented) A method for providing gated access for a third party to a secure entity or service comprising:

storing biometric data in dependence upon a biometric characteristic of a first designated user of the secure entity or service other than the third party;

storing biometric data in dependence upon a biometric characteristic of the third party;

capturing biometric information representative of a biometric characteristic and providing biometric data in dependence thereupon;

comparing the captured biometric data with the stored biometric data of the first designated user to produce a comparison result; and,

if the comparison result is indicative of a match:

providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service;

receiving the gating signal at the secure entity or service; and,

in response to the wireless gating signal, setting a flag within the secure entity or service, the flag for use in gating received wireless signals for controlling access to the secure entity or service such that in a first state the secure entity or service is non responsive to the wireless signals and in a second other state the secure entity or service is responsive to the wireless signals provided by the third party, the flag supporting a timing function such that the flag once set to the second other state returns to the first state after a predetermined, limited period of time absent additional comparison results indicative of a match.

5. (Previously presented) A method for providing gated access for a third party to a secure entity or service as defined in claim 4, comprising:

capturing biometric information representative of the biometric characteristic of the third party and providing biometric data in dependence thereupon;

comparing the captured biometric data with the stored biometric data of the third party to produce a comparison result; and,

if the comparison result is indicative of a match:

providing a wireless signal to the secure entity or service.

6. (Previously presented) A method for providing gated access for a third party to a secure entity or service as defined in claim 5, comprising providing access to the secure entity or service by the third party if the flag is in the second other state.

7. (Original) A method for providing gated access for a third party to a secure entity or service as defined in claim 5, wherein the third party comprises a plurality of persons.

8. (Original) A method for providing gated access for a third party to a secure entity or service as defined in claim 7, wherein different persons of the plurality of persons have different predetermined access privileges.

9. (Original) A method for providing gated access for a third party to a secure entity or service as defined in claim 8, comprising a plurality of different wireless signals associated with different persons of the third party having different access privileges.

10. (Original) A method for providing gated access for a third party to a secure entity or service as defined in claim 8, wherein the different predetermined access privileges comprise functional limitations of the secure entity or service.

11. (Previously presented) A method for providing gated access for a third party to a secure entity or service comprising:

providing to a first designated user other than the third party a first portable biometric device operable to capture biometric information presented thereto, the portable biometric device having stored biometric data in dependence upon a biometric characteristic of the first designated user;

providing the third party with a second other portable biometric device operable to capture biometric information presented thereto, the second portable biometric device having stored biometric data in dependence upon a biometric characteristic of the third party;

capturing biometric information representative of a biometric characteristic in response to the first designated user presenting said information to the first portable biometric device and providing biometric data in dependence thereupon;

comparing the captured biometric data with the stored biometric data in the first portable biometric device to produce a comparison result; and,

if the comparison result is indicative of a match, performing:

providing a wireless gating signal from the first portable biometric device for enabling wireless signals provided by the third party to access the secure entity or service;

receiving the gating signal at a port of the secure entity or service; and,

in response to the wire less gating signal, setting a flag within a locking mechanism of the secure entity or service, the flag for use in gating received wireless signals for controlling access to the secure entity or service such that in a first state the locking mechanism is non responsive to the wireless signals and in a second other state the locking mechanism is responsive to the wireless signals provided by the third party.

12. (Previously presented) A method for providing gaited access for a third party to a secure entity or service as defined in claim 11, comprising:

capturing biometric information representative of a biometric characteristic in response to the third party presenting said information to the second portable biometric device and providing biometric data in dependence thereupon;

comparing the captured biometric data with time stored biometric data in the second portable biometric device to produce a comparison result;

if the comparison result is indicative of a match, performing:

capturing biometric information representative of the biometric characteristic of the third party and providing biometric data in dependence thereupon;

comparing the captured biometric data with the stored biometric data of the third party to produce a comparison result; and,

if the comparison result is indicative of a match:

transmitting a wireless signal from the second portable biometric device to a port of the secure entity or service.

13. (Previously presented) A method for providing gated access for a third party to a secure entity or service as defined in claim 12, comprising providing access to the secure entity or service by the third party if the flag is in the second other state.

14. (Original) A method for providing gated access for a third party to a secure entity or service as defined in claim 12, wherein the wireless gating signal from the first portable biometric device and the wireless signal from the second portable biometric device are received at different ports of the secure entity or service .

15. (Original) A security system for securing an entity or a service from indiscriminate access and for providing gated access for a third party, the security system comprising:

at least a portable biometric device, the device comprising:

a biometric sensor for capturing biometric information representative of a biometric characteristic in response to a person presenting said information to the portable biometric device;

an encoder for digitally encoding the captured biometric information and providing biometric data in dependence thereupon;

memory for storing biometric data indicative of a biometric characteristic of

a first designated user;

a processor for comparing the captured biometric data with stored biometric data to produce a comparison result, and if the comparison result is indicative of the first designated user for providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service, and if the comparison result is indicative of the third party for providing a wireless signal;

a transmitter for wireless transmission of the wireless gating signal or the wireless signal;

at least a port for receiving the wireless gating signal and the wireless signal from the portable biometric device; and,

a locking mechanism for securing the entity or service, the locking mechanism comprising a processor for setting a flag in response to the wireless gating signal, the flag for use in gating received wireless signals for controlling access to the secure entity or service such that in a first state the locking mechanism is non responsive to the wireless signals and in a second other state the looking mechanism is responsive to the wireless signals provided by the third party.

16. (Original) A security system for securing an entity or a service from indiscriminate access as defined in claim 15, wherein the portable biometric device comprises memory for storing biometric data indicative of a biometric characteristic of the third party.

17. (Original) A security system for securing an entity or a service from indiscriminate to access as defined in claim 16, wherein the security system comprises a first portable biometric device for use by the first designated user and a second other portable biometric device for use by the third party.

18. (Original) A security system for securing an entity or a service from indiscriminate access as defined in claim 15, wherein the biometric sensor comprises a fingerprint imager.

19. (Original) A security system for securing an entity or a service from indiscriminate access as defined in claim 18, wherein the fingerprint imager comprises a capacitive fingerprint imager.

20. (Original) A security system for securing an entity or a service from indiscriminate access as defined in claim 15, wherein the locking mechanism comprises memory for storing data indicative of access privileges.

**9. EVIDENCE APPENDIX**

None.

**10. RELATED PROCEEDINGS APPENDIX**

None.

Date: June 12, 2006



---

Christos A. Ioannidi  
Registration No. 54,195

on behalf of Michael P. Dunnam  
Registration No. 32,611

Woodcock Washburn LLP  
One Liberty Place - 46th Floor  
Philadelphia PA 19103  
Telephone: (215) 568-3100  
Facsimile: (215) 568-3439

DOCKET NO.: IVPH-0049



PATENT

*22w*  
*AF#*

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**In Re Application of:**

Laurence Hamid, Derek Christopher Bouius  
and Albert Hum

**Confirmation No.:** 1343

**Application No.:** 09/863,301

**Group Art Unit:** 2135


**Filing Date:** May 24, 2001

**Examiner:** Thanhnga B. Truong

**For:** METHOD AND SYSTEM FOR PROVIDING GATED ACCESS FOR A THIRD  
PARTY TO A SECURE ENTITY OR SERVICE

DATE OF DEPOSIT: June 12, 2006

I HEREBY CERTIFY THAT THIS PAPER IS BEING  
DEPOSITED WITH THE UNITED STATES POSTAL  
SERVICE AS FIRST CLASS MAIL, POSTAGE PREPAID,  
ON THE DATE INDICATED ABOVE AND IS  
ADDRESSED TO THE COMMISSIONER FOR PATENTS,  
P.O. BOX 1450, ALEXANDRIA, VA 22313-1450.

  
TYPED NAME: Christos A. Ioannidi  
REGISTRATION NO.: 54,195

MS Appeal Brief - Patent  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**APPEAL BRIEF TRANSMITTAL  
PURSUANT TO 37 CFR § 41.37**

Transmitted herewith in triplicate is the APPEAL BRIEF in this application with respect to the Notice of Appeal received by The United States Patent and Trademark Office on **February 24, 2006**.

- ☐ Applicant(s) has previously claimed small entity status under 37 CFR § 41.37 .
- ☐ Applicant(s) by its/their undersigned attorney, claims small entity status under 37 CFR § 1.27 as:
- ☐ an Independent Inventor
  - ☐ a Small Business Concern
  - ☐ a Nonprofit Organization.

06/16/2006 MAHMED1 00000015 09863301

02 FC:1252

450.00 DP



- ☒ Petition is hereby made under 37 CFR § 1.136(a) (fees: 37 CFR § 1.17(a)(1)-(4) to extend the time for response to the Office Action of August 24, 2005 to and through June 12, 2006 comprising an extension of the shortened statutory period of two month(s).

	SMALL ENTITY		NOT SMALL ENTITY	
	RATE	FEE	RATE	FEE
<input checked="" type="checkbox"/> APPEAL BRIEF FEE	\$250	\$	\$500	\$500.00
<input type="checkbox"/> ONE MONTH EXTENSION OF TIME	\$60	\$	\$120	\$0.00
<input checked="" type="checkbox"/> TWO MONTH EXTENSION OF TIME	\$225	\$	\$450	\$450.00
<input type="checkbox"/> THREE MONTH EXTENSION OF TIME	\$510	\$	\$1020	\$0.00
<input type="checkbox"/> FOUR MONTH EXTENSION OF TIME	\$795	\$	\$1590	\$0.00
<input type="checkbox"/> FIVE MONTH EXTENSION OF TIME	\$1080	\$	\$2160	\$0.00
<input type="checkbox"/> LESS ANY EXTENSION FEE ALREADY PAID	minus	(\$ )	minus	(\$0.00)
TOTAL FEE DUE		\$0		\$950.00

- ☒ The Commissioner is hereby requested to grant an extension of time for the appropriate length of time, should one be necessary, in connection with this filing or any future filing submitted to the U.S. Patent and Trademark Office in the above-identified application during the pendency of this application. The Commissioner is further authorized to charge any fees related to any such extension of time to Deposit Account 23-3050. This sheet is provided in duplicate.
- ☒ A check in the amount of **\$950.00** is attached. Please charge any deficiency or credit any overpayment to Deposit Account No. 23-3050.
- ☐ Please charge Deposit Account No. 23-3050 in the amount of \$       .00. This sheet is attached in duplicate.
- ☒ The Commissioner is hereby authorized to charge any deficiency or credit any overpayment of the fees associated with this communication to Deposit Account No. 23-3050.

**DOCKET NO.: IVPH-0049**

**PATENT**

Date: June 12, 2006



Christos A. Ioannidi  
Registration No. 54,195

on behalf of Michael P. Dunnam  
Registration No. 32,611

Woodcock Washburn LLP  
One Liberty Place - 46th Floor  
Philadelphia PA 19103  
Telephone: (215) 568-3100  
Facsimile: (215) 568-3439

© 2006 WW